ICBC 中国工商银行（亚洲）

研究报告

Web3钱包技术基础及生态应用探讨

阅读摘要

Web3钱包作为连接用户与区块链网络的核心交互工具，是数字资产生态中最重要的基础设施之一，正朝着多链集成、身份认证与资产管理一体化的方向快速发展。本报告从内涵功能、技术分类、核心应用等维度系统梳理和探讨分析了Web3钱包发展现状与未来趋势。

欢迎扫码关注
工银亚洲研究

中国工商银行（亚洲）
东南亚研究中心
李卢霞 肖晶 徐麒钧
文晨宇 马爱莲 邹晓梦

Web3 钱包技术基础及生态应用探讨

一、Web3 钱包的内涵、功能与发展态势

（一）Web3 钱包的定义、特点与功能

从演进历程来看，**传统数字钱包**主要服务于 Web2.0 时代的移动支付场景，实现法币数字化及便捷交易；**Web3 钱包**则致力于成为下一代互联网（Web3.0）的“数字身份与资产管理中心”（见图表 1）。

图表 1：传统数字钱包 Vs Web3 钱包

	传统数字钱包 （Digital Wallet）	Web3 钱包 （Web3 Wallet）
核心功能	法定货币的数字化支付、存储支付凭证、线下扫码/NFC 支付	管理多元数字资产（加密货币、NFT 和其他数字资产）、与 DApp 交互、链上身份管理
主要技术	中心化服务器、加密技术、二维码、NFC	区块链公私钥体系、智能合约、跨链技术
典型代表	支付宝、微信支付、Apple Pay	MetaMask、Phantom、Trust Wallet
资产类型	账户余额信息等	加密货币、NFT、RWA 代币化资产等
控制权	由服务提供商中心化控制	用户自我托管，私钥自持
交互对象	银行、商家、支付网络	多条区块链、去中心化应用（DApp）、智能合约

数据来源：公开信息梳理、中国工商银行（亚洲）东南亚研究中心

Web3 钱包是连接用户与区块链网络的核心交互工具，也是数字资产生态中最重要的基础设施之一。其本质是一套基于公私钥加密体系的账户与身份管理系统，能够为用户生成、

存储和使用私钥，以实现对链上资产的完全控制与安全交易。与传统数字钱包、早期仅具备加密货币存储与转账功能的虚拟货币钱包不同，**目前的 Web3 钱包已演化为集资产管理、身份认证、应用入口和安全防护于一体的综合平台。**

Web3 钱包突出特征表现为两个方面：第一，大多数 Web3 钱包是自托管的（即用户自己掌握私钥，资产不由第三方控制），但部分交易所钱包（比如 Coinbase 钱包）或某些多链钱包，不一定是 Web3.0 原生钱包但支持某些 Web3.0 功能，甚至默认是“托管式”的。**第二，架构设计[1]上更注重应用层，**同时支持多链资产管理，使用户能够在统一界面轻松管理不同区块链上的资产，避免了传统多钱包切换的繁琐，大幅降低了使用门槛。

总结来看，**Web3 钱包核心功能可概括为三个方面：一是支持多资产和多链。**Web3 钱包支持多链、多资产的统一存储与估值管理，覆盖加密货币、稳定币、非同质化代币（NFT）、去中心化金融（DeFi）流动性凭证以及代币化现实世界资产（RWA）等多种类别。**二是跨场景应用连接。**促进与智能合约的无障碍交互，使用户能够访问去中心化应用（DApp）、去中心化交易平台（DEX）、其他基于区块链的应用程序，已成为用户连接 DeFi、GameFi、DAO、RWA 平台、链上治理等 Web3 场景的标准化通道。**三是跨生态身份认证。**Web3 钱包通过集成去中心化身份（DID）与链上声誉系统，使用户能

[1] 传统去中心化钱包通常由三层构成：密钥层(管理私钥的生成、导入导出以及签名生成)、地址层(按照主链格式生成地址)和应用层(用于资产管理，包括代币的转入和转出)。而 Web3 钱包更加注重应用层。

够在不同应用和生态中实现可验证、可携带的身份交互。

（二）Web3 钱包的市场规模快速增长，DeFi 是最活跃的应用赛道，新兴市场用户增速明显更高，热钱包收入占比过半

2024 年底日均独立活跃钱包总量近 2,500 万个，DeFi 板块钱包数量居首、占比近 1/3。截至 2024 年末，全球 Web3 用户规模[2]已突破 5.6 亿（约占全球人口的 6.8%）。**根据 DappRadar 数据统计，2024 年去中心化应用（DApp）生态的独立活跃钱包（UAW）总量全年增幅达 485%，至年末日均独立活跃钱包值（daily UAW）已升至 2,460 万个。**其中，DeFi 板块 UAW 同比扩张 532%，至 2024 年 12 月日均达到 700 万个，并于第四季度录得 32%的市场占有率，稳居细分赛道首位。回溯以太坊网络近十年历史累计数据，共计 2.34 亿个独立钱包曾与链上 DApp 发生交互，DeFi 以 74%的占比成为主要驱动领域，NFT、游戏及其他类别分列其后。

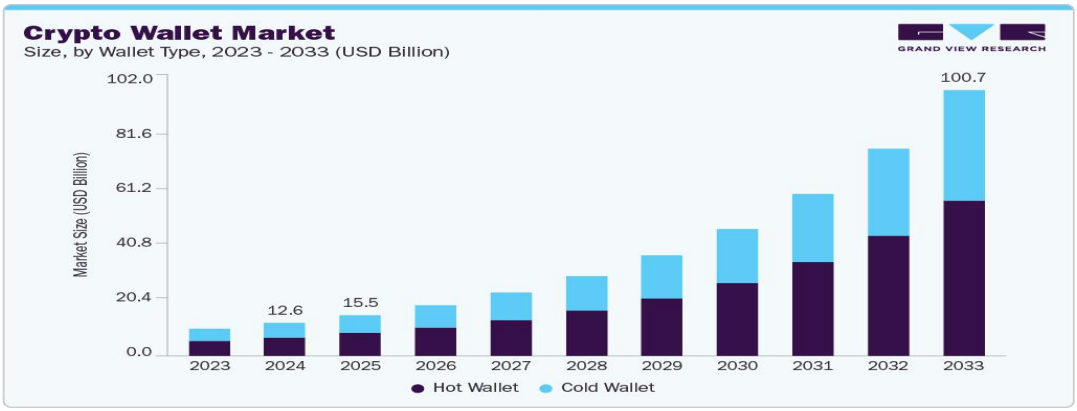
同时，**新兴市场（尤其是东南亚、拉丁美洲和非洲）的 Web3 钱包用户增长速度明显高于全球平均水平。**在传统金融基础设施覆盖不足的背景下，Web3 钱包因其“移动优先”的特性，被用作日常金融解决方案（如跨境转账、应对高通胀的理财工具），使用频率和应用深度迅速提升。

包括 Web3 钱包在内的加密钱包市场快速增长。根据 Grand View Research 的报告（见图表 2），到 2033 年，全

[2] 数据来源于 Triple-a 研报《The State of Global Cryptocurrency Ownership in 2024》。

球加密钱包市场收入份额规模预计将达到 1007.7 亿美元，年复合增长 26.3%。2024 年全球加密钱包市场规模估计为 125.9 亿美元。按钱包类型划分，**热钱包部分在 2024 年占据市场主导地位，收入份额为 56.0%。**

图表 2：全球加密钱包市场收入增长情况（百万美元, 2023-2033 年）



数据来源：Grand View Research、中国工商银行（亚洲）东南亚研究中心

（三）Web3 钱包市场格局呈现出头部集中趋势，链生态钱包在特定公链上形成高粘性用户基础

截至 2024 年末，全球 Web3 钱包市场呈现出头部集中趋势，MetaMask、Trust Wallet、Coinbase Wallet 等产品在活跃用户与生态覆盖方面保持领先，链生态钱包（Phantom、Tonkeeper）在特定公链上形成高粘性用户基础（见图表 3）。

图表 3：全球市占率排名前五的钱包情况

钱包名称	类型	活跃用户数(月活)	支持链生态	核心功能特点	主要优势
MetaMask	非托管	2000 万+	以太坊及 EVM 链	支持多链、DeFi/NFT 生态丰富、支持插件与移动端	1.全球最广泛使用的非托管钱包，月活 2000 万+; 2.深度绑定以太坊及 EVM 生态，兼容多链; 3.DApp 支持广泛，开发者生态强大; 4.浏览器插件与移动端双形态。

Trust Wallet	非托管	1000 万+	多链(EVM、BNB、Cosmos 等)	内置跨链、质押、NFT 管理等功能	1.支持多链(EVM、BNB、Cosmos 等),覆盖面广泛; 2.内置跨链与质押功能; 3.官方背书(Binance 生态)提升可信度; 4.移动端体验较好。
Coinbase Wallet	托管+非托管	800 万+	以太坊及 EVM 链	交易所生态整合、法币入口	1.支持托管与非托管双模式，兼顾安全与易用; 2.与 Coinbase 交易所无缝衔接，法币入口便利; 3.安全体系成熟，适合机构与新手。
Phantom	非托管	500 万+	Solana	原生支持 Solana DApp 与 NFT	1.原生支持 Solana 生态，速度快、体验流畅; 2.集成 NFT 管理与 DApp 入口; 3.社区活跃， Solana 用户首选。
Tonkeeper	非托管	300 万+	TON	原生支持 Telegram 生态与支付	1.原生绑定 TON 链与 Telegram 生态; 2.具有支付与社交场景天然优势; 3.门槛低，新用户容易上手。

数据来源：DappRadar、各钱包官网信息、中国工商银行（亚洲）东南亚研究中心

二、三个视角下的 Web3 钱包分类观察：特征及技术基础

（一）按私钥管理方式区分：中心化（托管）钱包和去中心化（非托管）钱包

按照私钥管理方式的不同，Web3 钱包可划分为托管钱包与非托管钱包两大类别。其中，**（1）中心化（托管）钱包**，多由交易所提供。该模式下，用户将数字资产交由平台托管，**其账户内显示的资产实质为交易所系统内部的记账凭证，用户并不实际持有私钥**，因而无法直接与去中心化应用（DApp）

交互。此类钱包的优势在于使用门槛低、操作简便，类似于传统银行账户，用户需信任服务商的安全机制。**Coinbase、币安、OKX、Hashkey Exchange 等交易所都提供托管钱包服务。（2）去中心化（非托管）钱包，**即自托管钱包，用户自行保管助记词和私钥，资产控制权完全归属用户。**钱包数据存储于用户本地设备，进行链上签名时由本地调用私钥完成。**这一模式赋予用户较充分自主权，但要求其承担更高安全管理责任，一旦助记词或私钥丢失或泄露，资产将无法恢复。**目前大多数 Web3 钱包专注于非托管解决方案。典型代表如 Metamask、Tonkeeper 钱包等。**

非托管钱包依技术实现可进一步分为三类：EOA 钱包、MPC 钱包和智能合约钱包。其中，**（1）EOA 钱包（**即 Externally Owned Account，典型代表如 MetaMask 钱包）是由私钥直接控制的外部账户钱包，通常通过助记词生成，若助记词遗失则资产无法找回。当用户发起交易（如转账、授权、交互 DApp）时，**钱包会在本地解密私钥，对交易数据进行签名，签名过程不依赖服务器，也不会泄露私钥。**但是，**传统的 EOA 钱包可能不支持复杂逻辑**[3]。

（2）MPC 钱包（即 Multi-Party Computation 钱包，典型代表如币安 Web3 钱包）通过安全多方计算技术将私钥分片，由多方共同参与管理，实现“无私钥”化存储。**交易发起时，各分片持有方通过链下多方计算协议协同生成有效签**

[3] MetaMask 用户可直接发起链上交易，无需通过智能合约逻辑。传统的 MetaMask 钱包不支持批量交易、社交恢复、Gas 代付等功能，后者往往是智能合约钱包具备的功能。2025 年，MetaMask 推出“智能账户”功能，允许用户将 EOA 升级为智能合约账户。

名，无需重构完整私钥。同时，**MPC 钱包可支持社交恢复、无助记词、多设备同步等功能**。但是，其安全性高度依赖于分片托管策略。

（3）智能合约钱包则通过智能合约管理账户，用户可自定义安全规则与操作逻辑。AA 钱包（即 Account Abstraction Wallet，典型代表如 Argent、Safe）就是智能合约钱包的一种实现形式，通过引入 ERC-4337 标准，将传统由私钥控制的 EOA 账户升级为智能合约控制的账户，从而拓展功能。ERC-4337 标准以 UserOperation 机制实现合约账户主动操作，令智能合约账户可像 EOA 钱包一样发起交易。

（二）按存储介质种类区分：软件钱包、硬件钱包和纸钱包

按照存储介质的不同，Web3 钱包主要可分为软件钱包、硬件钱包和纸钱包等类型。其中，**软件钱包**作为目前最主流的类型，以应用程序形式存在于计算机、智能手机或浏览器扩展中，用户通过下载并生成加密密钥来创建账户，私钥存储于设备本地。**此类钱包通常具备多链支持能力**，允许用户在单一界面内管理多种加密货币及 NFT，典型代表包括 MetaMask、Trust Wallet 等。

硬件钱包则通过物理设备提供更高层级的资产安全保障，其外形类似 USB 驱动器或小型电子设备，将私钥离线存储于硬件内部，可有效隔离网络攻击与恶意软件威胁。在进行交易签署时，硬件钱包需连接计算机或移动设备，所有签

名操作在设备内部完成，确保私钥不外泄。市场主流品牌如Ledger[4]、Trezor[5]等，具备广泛的区块链兼容性，适合需要高安全要求的用户和大额数字资产存储场景。

纸钱包作为一种较早的存储形式，是指将加密货币地址和私钥以物理方式打印或抄录于纸张之上进行离线保存。其优势在于完全隔绝网络风险，但同时也面临物理损坏、丢失或盗窃等问题。随着技术发展，纸钱包因使用不便、功能单一且容易失效，不再作为主流的钱包推荐类型。

（三）按是否联网区分：热钱包、冷钱包和暖钱包

热钱包与冷钱包是两类基础性产品形态，它们在技术架构、使用场景、安全性及目标用户等方面存在显著差异。其中：

热钱包依托互联网实时连接，能够为用户提供即时交易和链上交互的便利性，广泛用于日常转账、DeFi 操作、NFT 铸造与交易等高频链上活动。其优点在于便捷与高效，但因私钥存储于联网设备，受恶意攻击和钓鱼风险的潜在影响较大。

冷钱包则通过物理隔离或离线存储的方式保护私钥，通常以硬件钱包、纸钱包等形态存在，安全性显著高于热钱包，适合长期、大额资产的安全存放。

暖钱包，又称温钱包，是一种结合了热钱包的便捷性和

[4] Ledger 是法国专注于区块链安全技术的硬件钱包研发企业，其核心产品包括 Ledger Nano 系列硬件钱包及 Ledger Stax 等离线存储设备，通过物理隔离技术实现加密资产私钥的安全存储。

[5] 捷克程序员 Marek Palatinus 和 pavol Rusnak 于 2011 年构思、2013 年在布拉格成立公司 SatoshiLabs，2014 年正式发布全球首款比特币硬件钱包 Trezor One。2017 年，推出带彩色触控屏的 Trezor Model T。2023-2025 年，陆续发布 Trezor Safe 3 和 Trezor safe 5。截至 2025 年，Trezor 累计售出超百万台，与 Ledger、KeepKey 并列为“三大老牌硬件钱包”之一。

冷钱包的安全性的加密货币存储工具。在实际应用中，温钱包通过有限的网络连接和交易权限来平衡安全与便利，允许用户在在线和离线模式间切换的移动钱包。

图表 4：Web3 钱包类型

分类标准	子类别	描述	优缺点
联网	**冷钱包**	通过本地设备处理支付信息，其余不涉及安全问题的步骤联网完成。	优点：安全性高。 缺点：若为硬件钱包，造价相对较高。
	热钱包	联网钱包，所有交易联网进行。	优点：效率高。 缺点：安全隐患相对较高。
载体形态	**软件**	运行态（Running）程序[6]，有 APP、PC 客户端、浏览器插件等具体形式。	优点：效率相对较高。 缺点：安全隐患相对较大。
	硬件	使用单独的设备实现钱包功能，在专用硬件中执行密钥管理和密码学计算。	优点：安全性较高。 缺点：成本相对较高。
托管方式	**托管钱包**	托管在互联网上的数字钱包软件服务，由第三方平台（如交易所）管理私钥，用户只需要账户和密码就能访问。	优点：使用门槛较低，到账时间短，手续费低。 缺点：有潜在信用风险。
	非托管钱包	用户自己管理私钥。	优点：保护隐私、自主权大; 缺点：有被盗、丢失风险、效率低。

数据来源：公开信息梳理、中国工商银行（亚洲）东南亚研究中心

三、Web3 钱包的核心应用—如何“转账”？

“转账”是 Web3 钱包运作的基础功能。不同类型 Web3 钱包的创建步骤大体类似，但“转账”细节流程有一定差异。

（一）创建 Web3 钱包的三个步骤

第一步，生成私钥。在创建 Web3 钱包时，先随机生成

[6] 运行态（Running）程序是指正在 CPU 上执行，并占有 CPU 资源的程序，处于一个活跃的程序状态。

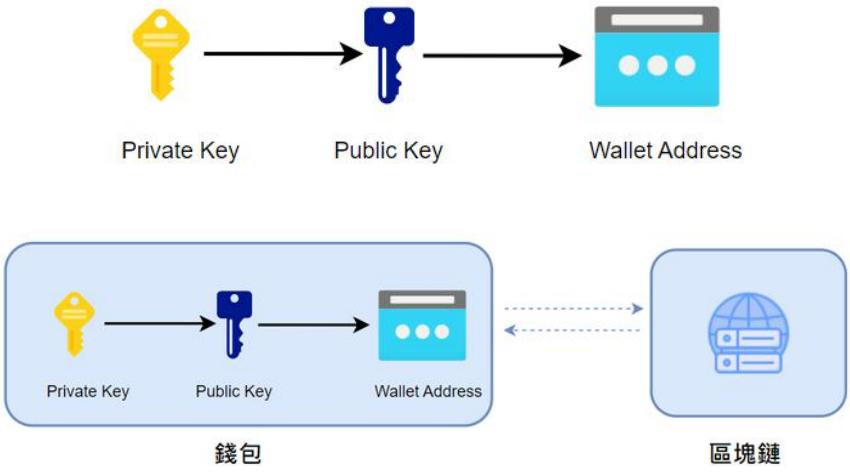
私钥，用于对数字资产进行签名，是一串复杂的随机字符、证明资产所有权。为便于使用，私钥通常会被转换为一组可读的**“助记词”**供用户备份。

第二步，生成公钥。公钥经私钥计算得出，但无法反向推导出私钥，即所谓的**“非对称加密”**。

第三步，创建 Web3 钱包地址。通过对公钥做哈希运算，可生成一个唯一的钱包地址，相当于用户的身份标识。

创建完成后，用户便可通过钱包地址进行身份验证，使用 DApps 提供的功能和服务，包括执行查询余额、发起交易、签署消息等操作。需要强调的两点：**一是用户可以创建多个钱包地址**，方便管理不同的数字资产，特别是不同链上资产。**二是钱包本身并不存储在区块链上，它只是一个管理密钥、协助用户与区块链交互的工具（见图表 5）。**

图表 5：钱包的创建路径以及钱包和区块链的关系



数据来源：公开信息、中国工商银行（亚洲）东南亚研究中心

（二）同链点对点转账：原生代币转账和智能合约代币

转账

对于在同一区块链上发生的交易，各钱包主要利用底层区块链的转账功能，其中包括原生代币转账以及智能合约代币转账。理论上，只需要知道对方的钱包地址，就可以发起转账交易，并需要为此支付 Gas 费用[7]。

1.原生代币转账：转账仅涉及普通地址交易。

原生代币（如比特币 BTC、以太坊 ETH）产生于独立的区块链网络，转账仅涉及普通地址交易，不涉及智能合约调用。交易中的数据涉及交易索引、交易金额、交易对手及交易成本等信息。**以 ETH 为例**，简单转账原理如下：

如通过软件钱包转账，以 MetaMask 为例，大致分为四个步骤：（1）**交易准备**，下载插件或 APP、安装&创建钱包；充值原生代币至 MetaMask 地址。（2）**发起交易**，在钱包内发起交易，输入对方地址、转账数量、选择 GAS 费；（3）**交易签名；**（4）**交易广播**。

如在硬件钱包内发起原生代币转账，以 Trezor 为例，也需四个步骤：（1）**连接钱包**，用 USB 把 Trezor 连接到电脑，打开 Trezor Suite；（2）**交易准备，**选择转账地址、转账数量、GAS 费；（3）**交易签名；**（4）**广播上链**。

2.智能合约代币转账：钱包负责构建交易和签名，“转账”由智能合约在链上完成。

智能合约代币（如 USDT）是基于智能合约的代币，在以

[7] Gas 费用是指在区块链上进行交易或执行智能合约时需要支付的费用，用于支付网络验证者处理交易的计算成本，并作为一种激励机制来维护区块链网络的安全性。

太坊网络中使用最为广泛，如 ERC-20 代币、ERC-721 代币等。**在以太坊上，只需知道对方钱包地址，即可发起转账交易，通过 ETH 支付 Gas 费用并执行智能合约**，工作原理如下:

（1）钱包软件内创建交易。在钱包软件中输入对方的钱包地址和转账金额，钱包会获取当前网络的 Gas 费等信息，草拟一笔待签名的交易。

（2）调用智能合约发起交易。通过调用以太坊 ERC-20 代币标准中定义的 Transfer()函数，将代币从一个地址转移到另一个地址。转账过程包括检查发送方的余额、指定接收方地址和转账金额[8]。

（3）私钥签名授权。上述交易信息会发送给用户的私钥进行签名。在这一过程中，用户并未直接暴露私钥，仅用私钥进行数字签，证明用户是该地址资产的合法所有者，并授权了这笔转账交易。

（4）钱包广播交易（上链）。签名后的交易被钱包发送（广播）到该区块链的网络中，矿工（或验证者）验证用户的签名是否有效，确认无误后将这笔交易打包进一个新的区块，从而永久记录在区块链上。此时，转账完成，对方钱包余额增加，发起方的余额相应减少。

本质上来看，同链转账并没有实际“移动”任何币。它只是在一个去中心化的公共账本（区块链）上更新了双方账

[8] Transfer 函数有两个参数，接收方地址和转移代币数量 Transfer（address to, Uint256 amunt）。Transfer 函数会在执行转移之前进行余额检查，若余额不足，转账会失败。

户的余额记录。用户的签名就是授权账本进行这次更新的唯一凭证。**钱包的角色是一个安全的指令构造器和签名器，而真正的资产转移逻辑则由智能合约在链上执行。**用户不是在“发送”代币，而是调用智能合约更新账本。

如使用硬件钱包调用智能合约转账，步骤类似，不同的是，把硬件钱包当做“冷签名器”使用。在此情形中，私钥存储于硬件设备，由电脑端配套软件完成合约调用、交易数据发送至硬件屏幕待确认，确认后设备离线签名，软件再把已签名交易广播上链。

（三）跨链转账：跨链桥、中继链、原子交换等是主流跨链技术方案

跨链转账指在不同区块链网络之间转移加密资产，由于不同区块链的运行逻辑和记账规则不同，**不同区块链上的数据无法直接交互**，因此需要在不同链之间建立可信桥梁，利用智能合约或中继机制来验证和执行跨链交易。根据信任模型和实现机制不同，**主流跨链技术方案包括跨链桥、中继链、哈希时间锁定（原子交换）等**。跨链转账可是同一用户不同链的钱包地址，也可是不同链上其他用户钱包地址。

1.跨链桥：本质上是 A 链锁定-B 链铸造（一币一链），跨链桥的智能合约和“中继器”负责交易监控。

本质是一种跨链消息传递协议，主要用于在不同区块链之间传输通证或资产。其原理通常是：在源链上通过智能合约锁定或销毁通证，然后在目标链上通过另一个智能合约解

锁或铸造。具体实现步骤如下:

（1）锁定资产。当用户发起跨链转账（例如，将 ETH 从以太坊转到 Solana），跨链桥会首先将 ETH 发送到它在以太坊上的一个智能合约地址，该合约会锁定（Lock）用户的 ETH。

（2）生成并映射资产。跨链桥在接收到资产已被锁定的证明后，会在目标链上铸造（Mint）一个等额的“映射资产”。这个映射资产通常是该链上的一种“封装资产”（如从以太坊来的 ETH 在 Solana 上会被映射为 soETH）。有些跨链桥（如 LayerZero、Wormhole）也致力于实现原生资产的跨链，但其底层逻辑依然是“锁定-铸造”或“销毁-铸造”。

（3）发放资产。新铸造的 soETH 会被发送到用户本人或另一用户在 Solana 链上指定的钱包地址。

（4）反向操作。如果用户想把 soETH 转回以太坊并恢复为原生 ETH 时，跨链桥会在 Solana 上销毁（Burn）用户的 soETH，并在证明销毁后，解锁最初在以太坊合约里锁定的 ETH，并将其发回地址。

跨链桥的智能合约和“中继器”（或“验证者”）负责监控链 A 的锁定事件，并在链 B 上触发铸造指令，是整个过程安全性的核心。

2. 中继链与子链：额外引入独立区块链作为中枢、负责验证子链状态或区块头摘要，中继链承担信任压力。

该方案引入一个独立的区块链作为中枢，该中枢负责连

接并协调所有接入的子链之间的跨链通信。**中继技术特别适用于将私有链或联盟链融入到公有链的共识网络中，同时又能保留其原有的数据隐私和许可使用的特性。**

具体工作原理如下：子链将自身状态或区块头摘要提交给中继链，中继链负责验证这些信息的有效性，从而确保跨链交易的可信性。这种架构将跨链的信任问题集中到了中继链上，降低了每条子链单独进行验证的成本和复杂性。

3．哈希时间锁定与原子交换：基于哈希时间锁定合约，本质上是确保两笔交易同时成功/失败，难以完成复杂的跨链资产交换。

哈希时间锁定合约是实现原子交换的核心机制，利用哈希锁和时间锁的组合，确保两笔在不同链上的交易要么同时成功，要么同时失败，从而保障交易的“原子性”。

其基本原理可以类比计算机处理器中的原子操作，如总线锁（Bus Lock）或比较并交换（CAS）。在处理器层面，这些机制通过独占内存或缓存的使用权，保证复杂的读-改-写操作不被其他处理器中断。整个过程不依赖任何第三方，从根本上保障了跨链交易的去中心化可信。

原子交换是实现去中心化资产互换的理想方案，主要局限性在于只支持简单的跨链资产交换，难以支持复杂的跨链智能合约调用和数据同步。

展望未来，Web3 钱包作为链接现实世界与 Web3 生态的核心入口，伴随基于区块链的跨境支付、RWA 交易快速发展，

将成为数字经济时代越来越重要的金融基础设施。

*免责声明

本报告由中国工商银行（亚洲）有限公司发出，以上条款建立在我行认为可靠信息的基础上，但我行并不表示对报告的准确或完整负责。如以上资料有所更改，我行恕不另行通知。上述资料仅供参考，我行并非借此诱导任何投资行为或预期未来利率／价格走势。我行或我行的任何关联机构可能拥有以上投资产品。

本报告并不构成我行作为上述交易及任何其他投资交易的顾问或令我行负上任何信托责任。我行不对报告或其内容运用负上任何法律责任。投资者在决定进行任何交易之前，应充分了解交易的详情和细则，并进行独立的分析，以评估该交易是否切合个人的条件和目标。我们也建议投资者作出独立的调查以达上述的目的。我行不保证或指示此投资产品将出现任何的投资结果。

这份报告是提供的资料仅供参考。本报告并不构成任何要约，招揽或邀请购买，出售或持有任何证券。投资价格可跌可升，投资者可能会损失部分或全部的投资。在本报告所载资料没有考虑到任何人的投资目标，财务状况和风险偏好及投资者的任何个人资料，因此不应依赖作出任何投资决定。订立任何投资交易前，你应该参照自己的财务状况及投资目标考虑这种买卖是否适合你，并寻求咨询意见的独立法律、财务、税务或其他专业顾问。

香港中資銀行業協會
Chinese Banking Association of Hong Kong

本文章发表的内容均为撰稿机构及/或作者的意见及分析，并不代表香港中资银行业协会意见。